

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-70377

(P2002-70377A)

(43) 公開日 平成14年3月8日 (2002.3.8)

(51) Int.Cl.	識別記号	F I	テ-マ-ト* (参考)
E 0 5 B 49/00		E 0 5 B 49/00	K 2 E 2 5 0
B 6 0 R 25/00	6 0 6	B 6 0 R 25/00	6 0 6
E 0 5 B 65/00		E 0 5 B 65/00	B
65/20		65/20	

審査請求 未請求 請求項の数 8 O L (全 6 頁)

(21) 出願番号 特願2000-266689(P2000-266689)

(22) 出願日 平成12年9月4日 (2000.9.4)

(71) 出願人 000006507

横河電機株式会社

東京都武蔵野市中町2丁目9番32号

(72) 発明者 胡 学良

東京都武蔵野市中町2丁目9番32号 横河

電機株式会社内

Fターム(参考) 2E250 AA02 AA03 AA21 BB08 BB59

BB65 CC28 CC29 DD01 FF24

FF34 FF36 HH01 JJ03 KK03

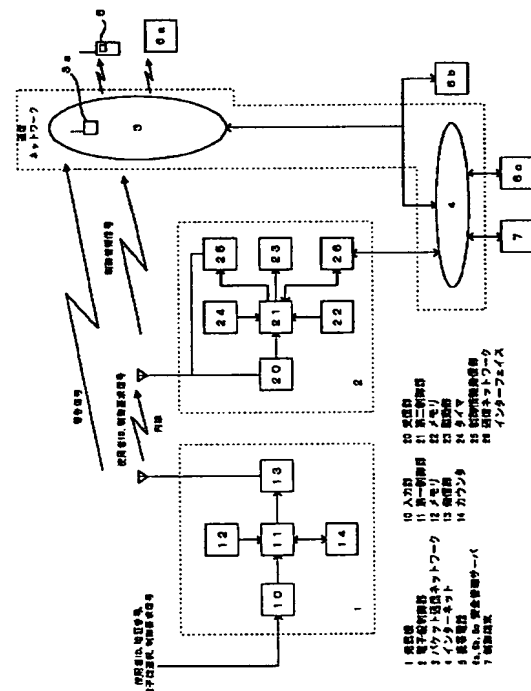
LL01 TT03

(54) 【発明の名称】 電子錠制御システム

(57) 【要約】

【課題】 セキュリティ性を高めて盗難などの犯罪被害を防止し、1台の発信機で複数の電子錠の施錠及び解錠を行うことができる電子錠制御システムを実現すること。

【解決手段】 電子錠と、発信機からの無線信号により電子錠を制御する電子錠制御機とを有する電子錠制御システムにおいて、発信機は、使用者ID、暗証番号及び制御要求信号が入力される入力部と、使用者IDと暗証番号との組み合わせが記憶されるメモリと、入力と組み合わせとが一致するか否か及び一致しない回数が所定回数以上であるか否かを判定する第一制御部と、一致する場合に使用者ID及び制御要求信号を電子錠制御機に発信すると共に、所定回数以上の場合に警告信号を外部に発信する発信部、とを具備し、電子錠制御機は、電子錠の駆動部と、受信部と、予め記憶された使用者IDと受信した使用者IDとが一致した場合に駆動部を駆動させる第二制御部、とを具備することを特徴とする電子錠制御システム。



【特許請求の範囲】

【請求項 1】 ドア、窓等の開閉部に設置された電子錠と、発信機から発信される無線信号を受信して前記電子錠の施錠及び解錠を行う電子錠制御機とを有する電子錠制御システムにおいて、

前記発信機は、

少なくとも前記発信機の利用者を識別する利用者 ID と、この利用者 ID を認証するための暗証番号と、前記電子錠の施錠または解錠を要求する制御要求信号とが入力される入力部と、

少なくとも一組の利用者 ID と暗証番号とが互に対応付けられた組合わせとして記憶されるメモリと、

前記入力部に入力された利用者 ID 及び暗証番号と前記組合わせとが一致するか否かを判定すると共に、一致しない回数が所定回数以上であるか否かを判定する第一制御部と、

前記入力部に入力された利用者 ID 及び暗証番号と前記組合わせとが一致すると判定された場合に前記利用者 ID 及び前記制御要求信号を前記電子錠制御機に発信すると共に、前記所定回数以上と判定された場合に警告信号を外部情報受信装置に発信する発信部、とを具備し、前記電子錠制御機は、

前記電子錠の施錠及び解錠を行う駆動部と、

前記発信部から発信された利用者 ID 及び制御要求信号を受信する受信部と、

予め記憶された利用者 ID と受信した利用者 ID とが一致した場合に前記制御要求信号に基づいて前記駆動部を駆動する制御信号を出力する第二制御部、とを具備することを特徴とする電子錠制御システム。

【請求項 2】 ドア、窓等の開閉部に設置された電子錠と、発信機から発信される無線信号を受信して前記電子錠の施錠及び解錠を行う電子錠制御機とを有する電子錠制御システムにおいて、

前記発信機は、

少なくとも前記発信機の利用者を識別する利用者 ID と、この利用者 ID を認証するための暗証番号と、前記電子錠の施錠または解錠を要求する制御要求信号とが入力される入力部と、

少なくとも一組の利用者 ID と暗証番号とが互に対応付けられた組合わせとして記憶されるメモリと、

前記入力部に入力された利用者 ID 及び暗証番号と前記組合わせとが一致するか否かを判定する第一制御部と、

前記入力部に入力された利用者 ID 及び暗証番号と前記組合わせとが一致すると判定された場合に前記利用者 ID 及び前記制御要求信号を前記電子錠制御機に発信する発信部、とを具備し、

前記電子錠制御機は、

前記電子錠の施錠及び解錠を行う駆動部と、

前記発信部から発信された利用者 ID 及び制御要求信号を受信する受信部と、

予め記憶された利用者 ID と受信した利用者 ID とが一致した場合に前記制御要求信号に基づいて前記駆動部を駆動する制御信号を出力する第二制御部と、

前記電子錠の制御情報信号を外部情報受信装置へ発信する制御情報発信部、とを具備することを特徴とする電子錠制御システム。

【請求項 3】 請求項 1 及び請求項 2 記載の電子錠制御システムにおいて、

前記発信機は、複数の前記電子錠制御機から選択された前記電子錠制御機に前記利用者 ID 及び前記制御要求信号を発信することにより、複数の前記電子錠から選択された前記電子錠の施錠及び解錠を行うようにしたことを特徴とする電子錠制御システム。

【請求項 4】 請求項 2 及び請求項 3 記載の電子錠制御システムにおいて、

前記制御情報信号は、前記電子錠が施錠または解錠された日時、前記利用者 ID、前記電子錠が施錠または解錠されたことを示す信号、選択された電子錠を識別する電子錠 ID の少なくとも一つを含むことを特徴とする電子錠制御システム。

【請求項 5】 請求項 1 から請求項 4 記載の電子錠制御システムにおいて、

前記利用者 ID、前記制御要求信号、前記警告信号及び前記制御情報信号はパケットデータとして発信されることを特徴とする電子錠制御システム。

【請求項 6】 請求項 2 から請求項 5 記載の電子錠制御システムにおいて、

前記警告信号及び前記制御情報信号は通信ネットワークを介して前記外部情報受信装置に通知されることを特徴とする電子錠制御システム。

【請求項 7】 請求項 1 から請求項 6 記載の電子錠制御システムにおいて、

前記発信機は、携帯電話または PHS 電話であることを特徴とする電子錠制御システム。

【請求項 8】 請求項 1 から請求項 7 記載の電子錠制御システムにおいて、

前記電子錠制御機は、前記第二制御部を前記通信ネットワークに接続する通信インターフェイスを具備し、前記通信ネットワークに接続された外部の制御機器より前記制御要求信号及び前記利用者 ID を前記第二制御部に入力するようにしたことを特徴とする電子錠制御システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えばドア、窓等の開閉部に設置された電子錠の施錠及び解錠を行う電子錠制御システムに関するものである。

【0002】

【従来の技術】従来、住宅店舗等の玄関ドア、自動車のドア、窓や金庫の扉等の開閉部に錠前を設け、開閉部に

設けられた鍵穴に対応する鍵を差し込んで回動させることにより、開閉部の施錠及び解錠が行なわれている。

【0003】そして、例えば玄関ドアの鍵を紛失してしまった場合、予め保管されていたスペアの鍵によって新しい鍵を作成して錠前を使用するようにしている。そして、スペアの鍵も紛失してしまった場合は、錠前を新規のものに交換するようにしている。

【0004】そして、鍵は開閉部に対して1対1で対応しているため、玄関ドア、自動車のドア等の複数の開閉部の施錠及び解錠を行う場合は、複数の鍵を携帯してその管理を行っていた。

【0005】

【発明が解決しようとする課題】しかし、このような鍵の管理においては次のような問題点があった。紛失した鍵が他者の手に渡ったり、鍵が偽造されたりした場合、財産の盗難の被害を受けたり、家族の人身の安全が危険にさらされる恐れがある。

(2) 鍵を紛失していない場合でも、開閉部に鍵穴があるため、鍵穴に特殊工具を差し込んで解錠させるピッキングと呼ばれる犯罪行為により、財産の盗難の被害を受けたり、家族の人身の安全が危険にさらされる恐れがある。

(3) 複数の鍵を携帯してその管理を行うことは煩雑であり、その負担が大きい。

【0006】本発明は上述した問題点を解決するためになされたものであり、開閉部に電子錠と電子錠の施錠及び解錠を行う電子錠制御機を設け、使用者ID及び暗証番号により認証された発信機から使用者ID及び電子錠の制御要求信号を特定の電子錠制御機を選択して発信し、選択された電子錠制御機において制御要求信号及びIDを受信し、IDが認証された場合に電子錠の施錠及び解錠を行うようにすることにより、セキュリティ性を高めて盗難などの犯罪被害を防止し、1台の発信機で複数の電子錠の施錠及び解錠を行うことができる電子錠制御システムを実現することを目的とする。

【0007】

【課題を解決するための手段】本発明の請求項1においては、ドア、窓等の開閉部に設置された電子錠と、発信機から発信される無線信号を受信して前記電子錠の施錠及び解錠を行う電子錠制御機とを有する電子錠制御システムにおいて、前記発信機は、少なくとも前記発信機の利用者を識別する使用者IDと、この使用者IDを認証するための暗証番号と、前記電子錠の施錠または解錠を要求する制御要求信号とが入力される入力部と、少なくとも一組の利用者IDと暗証番号とが互いに対応付けられた組み合わせとして記憶されるメモリと、前記入力部に入力された使用者ID及び暗証番号と前記組み合わせとが一致するか否かを判定すると共に、一致しない回数が所定回数以上であるか否かを判定する第一制御部と、前記入力部に入力された使用者ID及び暗証番号と前記組

わせとが一致すると判定された場合に前記使用者ID及び前記制御要求信号を前記電子錠制御機に発信すると共に、前記所定回数以上と判定された場合に警告信号を外部情報受信装置に発信する発信部、とを具備し、前記電子錠制御機は、前記電子錠の施錠及び解錠を行う駆動部と、前記発信部から発信された使用者ID及び制御要求信号を受信する受信部と、予め記憶された使用者IDと受信した使用者IDとが一致した場合に前記制御要求信号に基づいて前記駆動部を駆動する制御信号を出力する第二制御部、とを具備することを特徴とする電子錠制御システムである。

【0008】本発明の請求項2においては、ドア、窓等の開閉部に設置された電子錠と、発信機から発信される無線信号を受信して前記電子錠の施錠及び解錠を行う電子錠制御機とを有する電子錠制御システムにおいて、前記発信機は、少なくとも前記発信機の利用者を識別する使用者IDと、この使用者IDを認証するための暗証番号と、前記電子錠の施錠または解錠を要求する制御要求信号とが入力される入力部と、少なくとも一組の利用者IDと暗証番号とが互いに対応付けられた組み合わせとして記憶されるメモリと、前記入力部に入力された使用者ID及び暗証番号と前記組み合わせとが一致するか否かを判定する第一制御部と、前記入力部に入力された使用者ID及び暗証番号と前記組み合わせとが一致すると判定された場合に前記使用者ID及び前記制御要求信号を前記電子錠制御機に発信する発信部、とを具備し、前記電子錠制御機は、前記電子錠の施錠及び解錠を行う駆動部と、前記発信部から発信された使用者ID及び制御要求信号を受信する受信部と、予め記憶された使用者IDと受信した使用者IDとが一致した場合に前記制御要求信号に基づいて前記駆動部を駆動する制御信号を出力する第二制御部と、前記電子錠の制御情報信号を外部情報受信装置へ発信する制御情報発信部、とを具備することを特徴とする電子錠制御システムである。

【0009】本発明の請求項3においては、請求項1及び請求項2記載の電子錠制御システムにおいて、前記発信機は、複数の前記電子錠制御機から選択された前記電子錠制御機に前記使用者ID及び前記制御要求信号を発信することにより、複数の前記電子錠から選択された前記電子錠の施錠及び解錠を行うようにしたことを特徴とする電子錠制御システムである。

【0010】本発明の請求項4においては、請求項2及び請求項3記載の電子錠制御システムにおいて、前記制御情報信号は、前記電子錠が施錠または解錠された日時、前記使用者ID、前記電子錠が施錠または解錠されたことを示す信号、選択された電子錠を識別する電子錠IDの少なくとも一つを含むことを特徴とする電子錠制御システムである。

【0011】本発明の請求項5においては、請求項1から請求項4記載の電子錠制御システムにおいて、前記使

用者ID、前記制御要求信号、前記警告信号及び前記制御情報信号はパケットデータとして発信されることを特徴とする電子錠制御システムである。

【0012】本発明の請求項6においては、請求項2から請求項5記載の電子錠制御システムにおいて、前記警告信号及び前記制御情報信号は通信ネットワークを介して前記外部情報受信装置に通知されることを特徴とする電子錠制御システムである。

【0013】本発明の請求項7においては、請求項1から請求項6記載の電子錠制御システムにおいて、前記発信機は、携帯電話またはPHS電話であることを特徴とする電子錠制御システムである。

【0014】本発明の請求項8においては、請求項1から請求項7記載の電子錠制御システムにおいて、前記電子錠制御機は、前記第二制御部を前記通信ネットワークに接続する通信インターフェイスを具備し、前記通信ネットワークに接続された外部の制御機器より前記制御要求信号及び前記使用者IDを前記第二制御部に入力するようにしたことを特徴とする電子錠制御システムである。

【0015】

【発明の実施の形態】次に、本発明の実施例について図面を用いて説明する。図1は、本発明の実施例の構成概略図である。図1において、1は例えば携帯電話、PHS電話、発信機能を有する時計等の発信機、2は電子錠制御機、3は通信ネットワークとしてのパケット通信ネットワーク、4は通信ネットワークとしてのインターネット、5は外部情報受信装置としての携帯電話、6a、6b、6cは外部情報受信装置としての安全管理業者側に設置された安全管理サーバ、7は制御端末である。

【0016】発信機1及び電子錠制御機2は、電話の基本機能に加え、データ通信業者が構築しているパケット通信ネットワーク3を介したインターネット接続、電子メールの送受信等のパケットデータ通信を可能とする機能がデータ通信業者との契約により追加されている。

【0017】さらに、発信機1及び電子錠制御機2は、近距離データ通信用の無線通信インターフェイス規格に準拠したソフトウェア・スタックが実装されており、このソフトウェア・スタックは、パケット通信ネットワーク3を介することなく構内電話の内線やトランシーバのような使用を可能とするように規定された手法により実装されている。従って、発信機1と電子錠制御機2との間で構内電話の内線やトランシーバのように相互接続することが可能である。

【0018】また、発信機1がこの規格により無線通信インターフェイスとしてのソフトウェア・スタックが実装された機器であれば、どの発信機メーカーで製造されたものであっても、発信機1と電子錠制御機2との間で構内電話の内線やトランシーバのような相互接続が可能である。

【0019】そして、発信機1から電子錠制御機2に発信される電波の発信出力は、スペクトラム拡散通信技術のクラス3（最大転送距離10m）に対応するもので、その搬送波周波数は、2.4GHzのISM（Industrial Scientific Medical）帯を使用するので、その使用にあたって特別な免許は必要ない。

【0020】パケット通信ネットワーク3は、データ通信業者が構築している通信ネットワークであり、制御センター3aでパケットデータの送受信を行うことにより、発信機1または電子錠制御機2と、データ通信業者と契約している携帯電話5及び安全管理サーバ6aとの間のパケットデータの送受信を仲介する。

【0021】そして、パケット通信ネットワーク3は汎用の通信ネットワークとしてのインターネット4に接続されると共に、安全管理サーバ6bに専用線によって接続され、インターネット4には安全管理サーバ6cと制御端末7が接続されている。

【0022】次に、発信機の構成及び動作について説明する。発信機1は、入力部10、第一制御部11、メモリ12、発信部13、カウンタ14とから構成されている。尚、メモリ12及びカウンタ14は第一制御部11の内部に設けるようにしても良い。

【0023】使用者は、まず発信機1のパケットデータ通信メニューから電子錠制御モードを選択した後、入力部10に例えばプッシュボタン操作により発信機1の使用者ID、使用者の暗証番号を入力する。

【0024】メモリ12には、例えば家族構成員の使用者IDとそれに対応する暗証番号の組み合わせが複数個格納されており、第一制御部11は、入力部10に入力された使用者ID及び暗証番号と、メモリ12に格納された使用者ID及び暗証番号との組み合わせを比較する。

【0025】そして、それらが一致した場合、使用者は、例えば玄関ドアあるいは自動車ドア等の施錠または解錠の対象とする電子錠を選択して入力部10に入力し、発信部13は、選択された電子錠を識別する電子錠IDを内線またはトランシーバ等の手段により発信し、発信された電子錠IDに対応する電子錠に設けられた電子錠制御機2との相互接続を行う。

【0026】そして、使用者は、選択した電子錠の施錠または解錠を要求する制御要求信号を入力部10に入力し、発信部13は制御要求信号と使用者IDをパケットデータとして選択された電子錠に設けられた電子錠制御機2に内線またはトランシーバ等の手段により発信する。

【0027】一方、カウンタ14は、入力部10に入力された使用者ID及び暗証番号と、メモリ12に格納された使用者IDと暗証番号の組み合わせが不一致となった回数をカウントし、所定の回数として例えば連続して3回以上一致しない入力があった場合、第一制御部11は

不正な電子錠操作が試行されたと判断して警告信号を例えば電子メール等のパケットデータとして生成し、発信部 13 はこの警告信号を外部に発信する。

【0028】そして、発信された警告信号は、パケット通信ネットワーク 3 に接続された制御センター 3a で受信され、予め定められた携帯電話 5、安全管理サーバ 6a、6b、6c にパケット通信ネットワーク 3 及びインターネット 4 を介して通知される。

【0029】次に、電子錠制御機の構成及び動作について説明する。電子錠制御機 2 は、受信部 20、第二制御部 21、メモリ 22、開閉部に設けられた電子錠を解錠または施錠させる駆動部 23、タイマ 24、制御情報発信部 25、通信ネットワークインターフェイス 26 とからなっている。尚、メモリ 22 及びタイマ 24 は第二制御部 21 の内部に設けるようにしても良い。

【0030】メモリ 22 には、電子錠の制御を許す発信機 1 の複数の使用者 ID が予め記憶されており、受信部 2 は、発信機 1 から発信された電子錠 ID に応答して相互接続を行うと共に、使用者 ID 及び制御要求信号を受信し、第二制御部 21 は受信した使用者 ID とメモリに予め記憶されている使用者 ID とが一致するかどうかを判断し、一致する場合は、受信した制御要求信号に基づいて駆動部 23 を制御する制御信号を出力する。

【0031】そして、駆動部 23 は、第二制御部 21 の出力に基づいて、開閉部に設けられた電子錠を施錠または解錠させ、タイマ 24 は、駆動部 23 が電子錠を施錠または解錠した日時を検知して第二制御部 21 に出力する。

【0032】そして、制御情報発信部 25 は、タイマ 24 で検知された日時、使用者 ID、電子錠 ID、電子錠が施錠または解錠されたことを示す信号を電子錠の制御情報信号として、第二制御部 21 からの制御信号に基づいて外部に電子メール等のパケットデータとして発信する。

【0033】発信された制御情報信号は、パケット通信ネットワーク 3 に接続された制御センター 3a で受信され、パケット通信ネットワーク 3 及びインターネット 4 を介して予め定められた携帯電話 5、安全管理サーバ 6a、6b、6c に通知される。

【0034】そして、通信ネットワークインターフェイス 26 は、電子錠制御機 2 をインターネット 4 に接続するもので、外部の制御端末 7 は、インターネット 4 及び通信ネットワークインターフェイス 26 を介して電子錠の制御要求信号及び使用者 ID を第二制御部 21 に送信し、電子錠の施錠または解錠を行う。

【0035】そして、第二制御部 21 は、制御情報信号を安全管理データとして通信ネットワークインターフェイス 26 及びインターネット 4 を介して安全管理サーバ 6c に送信する。

【0036】また、家庭内のエアコン、風呂等の電気機

器をコントロールする小型サーバ（図示しない）を電子錠制御機 2 の内部に設けて受信部 20 と接続し、発信機 1 から電気機器をコントロールする制御信号を発信し、この制御信号を電子錠制御機 2 の受信部 20 で受信することにより、発信機 1 により電気機器のコントロールを行う、いわゆるホームオートメーションが可能となる。

【0037】また、電子錠制御機 2 に、バッテリーを内蔵させるか、あるいは発信機 1 からの電磁結合により電力を供給することにより、停電時にも電子錠を施錠及び解錠させることが可能となる。

【0038】また、電子錠制御機 2 に公衆電話回線との接続を行う公衆回線インターフェイス（図示しない）を設け、公衆電話回線を介して外部の公衆電話や設備電話等から使用者 ID 及び制御要求信号を入力することにより、データ通信業者の供給するパケットデータ通信システムが故障した場合でも電子錠の施錠及び解錠を行うことが可能となる。

【0039】上述のような電子錠制御システムによれば、発信機 1 と電子錠制御機 2 とは、内線、トランシーバ等によりパケット通信ネットワーク 3 を介さずに直接パケット通信を行うので通話料は発生せず、安価に電子錠の施錠及び解錠を行うことができる。また、スペクトル拡散通信技術により、他の無線通信からの干渉を受け難く、安定した電子錠の施錠及び解錠を行うことができる。

【0040】また、開閉部に鍵穴がないため、ピッキングによる盗難等の犯罪被害を防止することができる。また、一台の発信機で複数の電子錠の施錠及び解錠を行うことができるので、複数の鍵を携帯して管理する必要はない。

【0041】また、予め指定された携帯電話 5 及び安全管理サーバ 6a、6b、6c は警報信号や制御情報信号を受信することにより、その携帯電話 5 の使用者及び安全管理業者は、不正な電子錠操作が行われたことや、安全管理上必要なデータをリアルタイムに入手することができ、必要な対策を早急に講じることができる。

【0042】

【発明の効果】以上説明したように、本発明によれば、発信機の入力部に不正な使用者 ID 及び暗証番号が所定回数以上入力された場合に、発信機から警告信号を予め定められた携帯電話等の外部情報受信装置に発信するようにしたので、電子錠のセキュリティ性を高めて盗難などの犯罪被害を防止可能な電子錠制御システムを提供することができる。

【0043】また、本発明によれば、電子錠の施錠及び解錠が行われた場合に、電子錠の制御情報信号を電子錠制御機から予め定められた携帯電話等の外部情報受信装置に発信するようにしたので、電子錠のセキュリティ性を高めて盗難などの犯罪被害を防止可能な電子錠制御システムを提供することができる。

【0044】また、本発明によれば、発信機は、複数の電子錠制御機から選択された電子錠制御機に使用者ID及び制御要求信号を発信するようにしたので、1台の発信機で複数の電子錠の施錠及び解錠を行うことができる電子錠制御システムを提供することができる。

【0045】また、本発明によれば、制御情報信号を、施錠または解錠された日時、発信機の利用者ID、電子錠を識別する電子錠ID、電子錠が施錠または解錠されたことを示す信号としたので、電子錠のセキュリティ性を高めて盗難などの犯罪被害を防止可能な電子錠制御システムを提供することができる。

【0046】また、本発明によれば、利用者ID、制御要求信号、警告信号及び制御情報信号をパケットデータとしたので、データ通信業者の構築しているパケット通信ネットワーク、インターネット等の通信ネットワークを介して外部情報受信装置に発信することができる。

【0047】また、本発明によれば、発信機を携帯電話またはPHS電話としたので、汎用性のある電子錠制御システムを構築することができる。

【0048】また、本発明によれば、電子錠制御機に、通信ネットワークに接続する通信インターフェイスを設け、通信ネットワークに接続された外部の制御機器より

電子錠の制御要求信号及び利用者IDを直接電子錠制御機に入力可能としたので、パケット通信システムが故障した場合にも電子錠の施錠及び解錠を行うことができる。

【図面の簡単な説明】

【図1】本発明の実施例の構成概略図である。

【符号の説明】

- 1 発信機
- 2 電子錠制御機
- 3 パケット通信ネットワーク
- 4 インターネット
- 10 入力部
- 11 第一制御部
- 12 メモリ
- 13 発信部
- 20 受信部
- 21 第二制御部
- 22 メモリ
- 23 駆動部
- 24 制御情報発信部
- 26 通信ネットワークインターフェイス

【図1】

